Results for "(('portable device' and password)<in>metadata)" e-mail
Your search matched 1 of 1318251 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(('portable device' and password)<in>metadata) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **Parasitic authentication to protect your e-wallet**
Ebringer, T.; Thorne, P.; Zheng, Y.;
Computer
Volume 33, Issue 10, Oct. 2000 Page(s):54 - 60
Digital Object Identifier 10.1109/2.876293
AbstractPlus | References | Full Text: PDF(404 KB) IEEE JNL
Rights and Permissions

Terms used **portable device password** Found **53** of **171,143**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 53 Result page: **1** 2 3 next

Relevance scale

1 Satchel: providing access to any document, any time, anywhere

Mik Lamming, Marge Eldridge, Mike Flynn, Chris Jones, David Pendlebury
September 2000 **ACM Transactions on Computer-Human Interaction (TOCHI)**, Volume 7 Issue 3
Publisher: ACM Press

Full text available: pdf(591.29 KB) Additional Information: full citation, abstract, references, citings, index terms

Current solutions for providing access to electronic documents while away from the office do not meet the special needs of mobile document workers. We describe "Satchel," a system that is designed specifically to support the distinctive features of mobile document work. Satchel is designed to meet the following five high-level design goals (1) easy access to document services; (2) timely document access; (3) streamlined user interface; (4) ubiquity; and (5)compliance with securi ...

Keywords: document access, document appliance, document processing, information appliance, mobile computing, mobile work

2 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press

Full text available: pdf(306.59 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

3 A composable framework for secure multi-modal access to internet services from Post-PC devices

Steven J. Ross, Jason L. Hill, Michael Y. Chen, Anthony D. Joseph, David E. Culler, Eric A. Brewer

October 2002 **Mobile Networks and Applications**, Volume 7 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(340.33 KB) Additional Information: full citation, abstract, references, index terms, review

The Post-PC revolution is bringing information access to a wide range of devices beyond the desktop, such as public kiosks, and mobile devices like cellular telephones, PDAs, and voice based vehicle telematics. However, existing deployed Internet services are geared toward the secure rich interface of private desktop computers. We propose the use of an infrastructure-based secure proxy architecture to bridge the gap between the capabilities of Post-PC devices and the requirements of Internet ser ...

Keywords: internet, middleware, post-PC, security, transcoding

4 Cases from the field: Where am I and who am I?: issues in collaborative technical help

Michael Twidale, Karen Ruhleder

November 2004 **Proceedings of the 2004 ACM conference on Computer supported cooperative work**

Publisher: ACM Press

Full text available: pdf(296.47 KB) Additional Information: full citation, abstract, references, index terms

In a study of collaborative help-giving within several organizations settings, we identified two forms of trouble and bewilderment that we explore further in this paper. In one case, the user is confused about where they, their files, or other resources are within a larger technical infrastructure (Where am I?). In the second case, the user isn't sure which login is needed and which actions are allowed (Who am I?). We believe that these issues carry important implications for the design of in ...

Keywords: CSCW, collaborative help-giving, informal learning

5 A service management framework for M-commerce applications

Gary Shih, Simon S. Y. Shim

June 2002 **Mobile Networks and Applications**, Volume 7 Issue 3

Publisher: Kluwer Academic Publishers

Full text available: pdf(650.12 KB) Additional Information: full citation, abstract, references, citings, index terms

Mobile commerce (m-commerce) refers to an ability to conduct wireless commerce transactions using mobile applications in mobile devices. M-commerce applications can range from as simple as an address book synchronization to as complicated as credit card transactions. M-commerce is expected to grow dramatically in the near future supporting simple to complex commerce transactions. Even though the Wireless Application Protocol (WAP) is designed to facilitate the development of wireless application ...

Keywords: JINI, WAP, m-commerce, management, mobile devices

6 Personalizing shared ubiquitous devices

David M. Hilbert, Jonathan Trevor

May 2004 **interactions**, Volume 11 Issue 3

Publisher: ACM Press
Full text available: pdf(4.04 MB) html(48.57 KB) Additional Information: full citation, references, index terms

7 Mobile services: Reincarnating PCs with portable SoulPads
Ramón Cáceres, Casey Carter, Chandra Narayanaswami, Mandayam Raghunath
June 2005 **Proceedings of the 3rd international conference on Mobile systems, applications, and services MobiSys '05**
Publisher: ACM Press
Full text available: pdf(199.97 KB) Additional Information: full citation, abstract, references

The ability to walk up to any computer, personalize it, and use it as one's own has long been a goal of mobile computing research. We present *SoulPad*, a new approach based on carrying an auto-configuring operating system along with a suspended virtual machine on a small portable device. With this approach, the computer boots from the device and resumes the virtual machine, thus giving the user access to his personal environment, including previously running computations. *SoulPad* ha ...

8 Your place or mine?: privacy concerns and solutions for server and client-side storage of personal information
Deirdre Mulligan, Ari Schwartz
April 2000 **Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions**
Publisher: ACM Press
Full text available: pdf(83.62 KB) Additional Information: full citation, references, index terms

9 Copyrights and access-rights: How DRM-based content delivery systems disrupt expectations of "personal use"
Deirdre K. Mulligan, John Han, Aaron J. Burstein
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(416.68 KB) Additional Information: full citation, abstract, references, index terms, review

We set out to examine whether current, DRM-based online offerings of music and movies accord with consumers' current expectations regarding the personal use of copyrighted works by studying the behavior of six music, and two film online distribution services. We find that, for the most part, the services examined do not accord with expectations of personal use. The DRM-based services studied restrict personal use in a manner inconsistent with the norms and expectations governing the purchase and ...

Keywords: access control, content distribution, copyright, digital rights management, fair use, personal use, privacy

10 Efficient Web form entry on PDAs
Oliver Kaljuvee, Orkut Buyukkokten, Hector Garcia-Molina, Andreas Paepcke
April 2001 **Proceedings of the 10th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(398.94 KB) Additional Information: full citation, references, citings, index terms

Keywords: PDA, WAP, forms, mobile computing, wireless access

11 Stuck in nerdville: implementing a laptop checkout program via information commons

Amanda Moos, Chad Talbert
October 2004 **Proceedings of the 32nd annual ACM SIGUCCS conference on User services**
Publisher: ACM Press
Full text available: pdf(171.65 KB) Additional Information: full citation, abstract, references, index terms

Keeping up with the children of the 'now' generation, requires variety, entertainment, and the 'wow' effect. They require information fast, frequent, and at their fingertips. They want to be mobile and online at the same time. While the provision of wireless networking, a common trend among higher learning institutions, has done a decent amount of progress, it does not provide equal access to all. How do we address the demands of this generation when some of them don't own a laptop/computer, ...

Keywords: 1x authentication, check-in, check-out, environment, information commons, lab consultants, laptop checkout program, laptops, library, portability, traditional computing lab, wireless networking

12 Articles: UbiData: requirements and architecture for ubiquitous data access

Abdelsalam Helal, Joachim Hammer
December 2004 **ACM SIGMOD Record**, Volume 33 Issue 4
Publisher: ACM Press
Full text available: pdf(223.13 KB) Additional Information: full citation, abstract, references

Mobile users today demand ubiquitous access to their data from any mobile device and under variable connection quality. We refer to this requirement as *any-time, any-where* data access whose realization requires much more support for asynchronous and disconnected operation than is currently available from existing research prototypes or commercial products. Furthermore, the proliferation of mobile devices and applications, forges the additional requirement of device- and application-transp ...

13 Trends for 2005

Aaron Weiss
December 2004 **netWorker**, Volume 8 Issue 4
Publisher: ACM Press
Full text available: pdf(80.15 KB) html(29.15 KB) Additional Information: full citation, abstract, index terms

A fractured landscape of technological innovations reveals that now, more than ever, we're all connected

14 Industry presentations: Mobile device security

Benjamin Halpert
October 2004 **Proceedings of the 1st annual conference on Information security curriculum development**
Publisher: ACM Press
Full text available: pdf(49.69 KB) Additional Information: full citation, abstract, references, index terms

Because of their small size, memory capability, and the case with which information can be downloaded and removed from a facility, mobile devices pose a risk to organizations when used and transported outside physical boundaries. Mobile devices, including Personal Digital Assistants (PDAs), mobile phones, laptops, and smart phones can expose organizational data if not properly protected. This paper will cover areas of concern, different device types, and proposed solutions to mitigate the risks ...

Keywords: PDA, encryption, laptop, mobile, security

15 Papers from MC²R open call: Condor grid computing from mobile handheld devices

Francisco J. González-Castaño, Javier Vales-Alonso, Miron Livny, Enrique Costa-Montenegro, Luis Anido-Rifón

January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(2.65 MB) Additional Information: full citation, abstract, references

In this paper, we propose a hierarchical design methodology for grid access from handheld devices. After determining all user interactions required and technologies available, they are arranged in layers. All functions in a layer are also supported by all underlying layers. By doing so, the designer is less conditioned by the constraints of a specific, out-of-context platform. Additionally, in a stratified modular design, many software components can be re-used. We present a prototype to access ...

16 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation**

Publisher: ACM Press

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

***Keywords**: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

17 People, places, things: web presence for the real world

Tim Kindberg, John Barton, Jeff Morgan, Gene Becker, Debbie Caswell, Philippe Debaty, Gita Gopal, Marcos Frid, Venky Krishnan, Howard Morris, John Schettino, Bill Serra, Mirjana Spasojevic

October 2002 **Mobile Networks and Applications**, Volume 7 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(248.58 KB) Additional Information: full citation, abstract, references, citings, index terms, review

The convergence of Web technology, wireless networks, and portable client devices provides new design opportunities for computer/communications systems. In the HP Labs'

"Cooltown" project we have been exploring these opportunities through an infrastructure to support "web presence" for people, places and things. We put web servers into things like printers and put information into web servers about things like artwork; we group physically related things into places embodied in web servers. Using ...

Keywords: location-aware computing, nomadic computing, physical-virtual linkage, ubiquitous computing, world wide web

18 MARE: resource discovery and configuration in ad hoc networks

Matt Storey, Gordon Blair, Adrian Friday

October 2002 **Mobile Networks and Applications**, Volume 7 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(246.73 KB) Additional Information: full citation, abstract, references, index terms

The emergence of personal portable devices, such as PDA's and Mobile phones, with considerable processing and communication capabilities, has led to a desire to use various combinations of these devices together to achieve new and as yet unrealised operations. Not only are mobile devices expected to offer conventional facilities like email and web browsing but also more demanding multimedia applications. Attaining these operations within a fixed network environment with high-power workstations i ...

Keywords: ad hoc, mobile agents, resource discovery, tuple space

19 Client-server computing in mobile environments

Jin Jing, Abdelsalam Sumi Helal, Ahmed Elmagarmid

June 1999 **ACM Computing Surveys (CSUR)**, Volume 31 Issue 2

Publisher: ACM Press

Full text available: pdf(233.31 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Recent advances in wireless data networking and portable information appliances have engendered a new paradigm of computing, called mobile computing, in which users carrying portable devices have access to data and information services regardless of their physical location or movement behavior. In the meantime, research addressing information access in mobile environments has proliferated. In this survey, we provide a concrete framework and categorization of the various way ...

Keywords: application adaptation, cache invalidation, caching, client/server, data dissemination, disconnected operation, mobile applications, mobile client/server, mobile compuing, mobile data, mobility awareness, survey, system application

20 Condor grid computing from mobile handheld devices

Francisco J. González-Castaño, Javier Vales-Alonso, Miron Livny, Enrique Costa-Montenegro, Luis Anido-Rifón

April 2002 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 6 Issue 2

Publisher: ACM Press

Full text available: pdf(199.54 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we propose a hierarchical design methodology for grid access from handheld devices. After determining all user interactions required and technologies available, they are arranged in layers. All functions in a layer are also supported by all underlying layers. By doing so, the designer is less conditioned by the constraints of a specific, out-of-context platform. Additionally, in a stratified modular design, many

software components can be re-used. We present a prototype to access ...

Results 1 - 20 of 53 Result page: **1** 2 3 next

Access Control for Future Mobile Devices

Hongyuan Chen, and T.V.L.N Sivakumar

Nokia Research Center Japan
Arco Tower, 1-8-1 Shimomeguro, Meguro-ku, Tokyo 153-0064
{hongyuan.chen,t.sivakumar}@nokia.com

Abstract— Mobile wireless communications will be more and more important in our life, thus, how to control the access to our mobile devices become crucial. This paper proposes a method to access the mobile device and through the device to access Internet. We classify the usernames and passwords necessary for accessing web accounts as well as the personal documents and information stored in the mobile device into a few groups according to the importance of the corresponding contents protected by them. The contents protected by usernames and passwords in one group are ideally of same importance, and an authenticating method is used to access them. For more important group, authenticating method with higher security level is needed to access. User authenticates to her/his mobile device using fingerprint, high security password or normal password, and then she/he can not only access corresponding groups of information stored in the device but also use that device to access corresponding groups of her/his web accounts seamlessly without memorizing usernames and passwords. Different authentication methods represent different security levels. Whenever the user wants to access information stored in the mobile devices, or web accounts provided by a third party, the security middleware obtains security levels required to access them, compares the requirements with the authenticated security level. If the authenticated security level is equal to or higher than the requirements, the access is granted seamlessly and transparently to the user; otherwise, it asks to authenticate again using corresponding security level or higher, or the access is denied. After the access right to a device is granted, the user can at any time reset the access, or the access can be reset automatically after a predefined idle period. To gain the access again, the user needs to repeat the same authentication process as s/he did at the first time to access the device.

***Index Terms*—Access control, Authentication, Fingerprint, Password, Multi-level access, Smart card**

I. INTRODUCTION

As computing power of mobile devices becomes more and more powerful, there will be a natural trend that more and more resource intensive services will also be accessed through these devices because of the inherent advantages, and conveniences offered by portable devices. In line with these changes, mobile devices such as mobile phones, and PDAs turn into versatile all in one personal service managers: They can be used for paying money, accessing contents, services, and applications provided via the Internet, controlling home electronics and storing personal and important business data etc. Therefore, it is very important to ensure strict access control to the data both on the device, and through the device. Since importance of data items varies significantly, it is required that access control mechanisms reflect these requirements rather than implement a simple one solution that fits all requirements. More over, these mechanisms need to be sufficient, intuitive, and user friendly in order to encourage their use rather than minimize their use.

In order to access contents and services provided by third parties via the Internet, usernames and passwords are needed for the purpose of authentication. In general, the importances of data items protected by those usernames and passwords can be divided into a few groups such as every high, high, middle and low. For data items in many accounts, their importances are the same although different usernames and passwords are applied to protect them. For example, in order to access a web page that provides scientific article searching service, a user needs username1 and password1 to sign in; in other cases, the same user needs username2, password2, username3, password3 and so on to download music, to read phone bill information, to get after sale services for electronic products etc. These username and password pairs are of same security level for the user, but she/he has to remember them and provide them correctly while using them. The number of usernames and passwords that a user needs to remember tend to increase rapidly as our society and life go "electronic" or "on-line". It is already a heavy burden for users to remember usernames and passwords, and it will become worse year-by-year. The situation is further serious as many web accounts request users changing their passwords frequently. Although this problem can be made easy by giving the same username and password to all accounts or rotating them among a few pairs as some users have already done [1], however, by doing so the overall security of all accounts is degraded because one password been hacked will cause free access in many accounts authenticated by that password.

This paper proposes a novel access control for both mobile terminal access, and contents and service access outside the terminal via wired and wireless world. The rest of the paper is organized as following. Section 2 gives the background of the current research works. Then our novel access control method and its implementation are described in Section 3 and Section 4 respectively. The performance of our proposal is analyzed in Section 5. Finally we present the conclusions in Section 6.

II. BACKGROUND

As we take the advantages of "e-society" and "e-life", we also have to encounter many new challenges. One of them may be proving our identity everywhere in the e-world. The most commonly employed mechanism is by substituting the identity with username, and password pairs. The identity proving not only challenges the traditional privacy policy [2], which is not the issue of this paper, but also confuses people with so many usernames and passwords that are difficult to be remembered. Therefore, users tend to choose usernames and passwords that are easy to remember and to use the same username and password for many accounts or several sets of usernames and passwords everywhere.

Persistent cookies [3] is a widely used method that eases the password memorization problem. When a user submits a username and password to a Web server to create an account, the Web server can encode them as cookies and send them back to the user's Web browser using a "set-cookie" instruction in the header of the HTTP response message; the Web browser then saves them in a file on the user's computer. Later on, when the user accesses the account, the Web browser automatically submits all cookies that were previously set by the Web server, including the encoded username and password, using a "cookie" instruction in the header of the HTTP request message. The Web server then authenticates the user based on the submitted cookies. With help of cookies, the user does not have to remember any password, and even does not need to enter them manually as long as he/she uses the same computer. However, this method has the following weaknesses: (1) the user cannot access an account using another computer if forgetting the username and password of that account; (2) a security breach could occur if the user shares the computer with others; and (3) it does not guarantee password independence among multiple accounts.

Another method to solve the password memorization problem is proxy-based services, such as the Passport service from Microsoft. A user does not need to create individual accounts on e-commerce Web servers associated with the Passport service; instead, the user only establishes one account at the Passport server (and therefore remembers only one username and password), and saves personal financial information into it. When checking out at an e-commerce Web server, the user needs to click on a Passport logo presented by the e-commerce Web server. The Passport authentication page is then downloaded to the user's Web browser. After the user submits the username and password, the Passport server retrieves the user's financial data from the account database and forwards it to the e-commerce Web server. Although the Passport service provides convenience and some degree of security assurance for users in Web-based transactions, it does not completely solve the password memorization problem. A user still needs to open individual accounts on e-commerce Web servers that are not associated with the Passport server, or open other types of accounts that are not for e-commerce. Even worse, if a user uses the same username and password to protect the account at the Passport server and any other account at any other server, a hacker can steal them using a malicious server attack, and then impersonate the user to fool every e-commerce Web server associated with the Passport server.

Liberty Identity Federation Framework (ID-FF) [4] is similar to passport service. It is a multi-vendor, Web-based single sign-on with simple federated identities. At first, businesses affiliate together into *circles of trust* based on Liberty-enabled technology and on operational agreements that define *trust relationships* between the businesses. Secondly, users federate the isolated accounts they have with these businesses (known as their *local identities*) by a process of introduction. Such an introduction is the means by which a service provider may discover which identity providers in the circle of trust have authenticated the user. In other words, a circle of trust is a federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.

Luo and Henry [5] proposed a common password to access multiple accounts. Each account is protected by a different password, called a specific password that is stored at the account server or a proxy in an encryption form, where the encryption key is derived from the common password. Compared with a convenient hut insecure practice of using one or several passwords to protect multiple accounts, it assures that compromising one specific password does not reveal the common password and any other specific password. However, it is difficult to change the common password because it affects all specific passwords, and the loss of common password makes it impossible to access all specific passwords.

III. ACCESS CONTROL MECHANISM

Even at this stage of mobile communications development, many mobile centric transactions are happening, and life is going mobile. Nowadays, users normally access web accounts through mobile devices by providing login usernames and passwords. It may not be surprising that in the near future each user may have to keep several tens of usernames and passwords or even more, and they have also to change the passwords frequently for fulfilling security obligations. Although the existing methods described in Section 2 may be modified for use in future versatile mobile devices, they may still have reported inconveniences in accessing both devices, and services through the devices. In order to improve security and to free users from memorizing variety of passwords, we propose a novel access control method to seamlessly access all web accounts without inputting the necessary usernames and passwords each time at login. Our proposal also provides multi-level accesses for multiple users. For example, when the mobile device is used as remote controller at home, everyone in the home can use it; for family members, they may allowed to order pay TV programmes using the mobile device etc.

Our method consists of two steps: preparation and real-time access control.

A. Preparation

In preparation, all username and password pairs are divided into a few groups. Username and password pairs in the same group are of same security levels, which means that the importances of the contents, services and applications protected by them are of the same level. Username and password groups are stored in the smart card of the mobile device. Meanwhile, an

authentication method required to gain access to each group is determined. For personal documents and information stored in the mobile device, the same classification rule is applied. Table 1 illustrates an example of assigning security levels to contents, services and applications, where Web represents the web address to access the content or service, U and P mean the username and password to login to that web account, and App is the entry to the application that provides the control or information specified in the left column. Additionally each authentication method, and/or security level has a timeout mechanism to guard against prolonged misuse of the stolen or misplaced devices.

Table 1. Example of assigning security levels to contents, services and applications

Security level	Required authen. to gain access	Contents, services & applications	Access method
L1	Fingerprint + L1 password	Bank account management	Web1-10/U1-10/P1-10
		Stock and finance management	Web11-20/U11-20/P11-20
		Modify data in smart card, password update.	App1, App2
L2	Fingerprint	Small amount of money payment, payments by credit cards	P30
		Sensitive personal information	P40
		Home/office access and security control	App3
L3	L3 password or fingerprint	Confidential documents	Web50/U50/P50
		Important data	Web60/U60/P60
		Secure applications	App4
		Home/personal network control/access	App5
L4	L4 or L3 password or fingerprint	Contents, services, applications that are not confidential, but are not freely accessible to others	Web61-80/U610-80/P61-80
		Restricted controls, e.g. paid TV channels	App11-20
L5	Free access (no authen. needed.)	Free contents, services, applications that can be accessed or downloaded by everyone. Ordinary phone and email functions. Remote control of home electronics, e.g. TV, video, air conditioner etc.	Web81-99 App21-30

According to the example given in Table 1, totally a user needs to remember three passwords. For simplification, row L4 can be merged into rows of L3 and L5 to reduce the total security levels to 4 and the passwords needed to remember to two. In fact, if a user uses his own mobile device, he needs only to remember the L1 password, because he can access all L2 to L5 information using fingerprint authentication. L3 and L4 passwords are needed only when the owner share his mobile device with other users.

The contents, services and applications in L1 are the most important ones; therefore, they are most strongly protected. To access bank accounts, for example, the user needs to provide L1 password after a successful fingerprint authentication. L1 password is necessary for protecting the accesses beyond the owner's will, for example, in hostile environment.

B. Real-time access control

A user first authenticates to get control to his mobile device, and then uses the mobile device to access internal and external contents, services and applications. The standard authentication algorithms can be used for user authentication. For example, the fingerprint authentication algorithms described in [6][7][8] and the password authentication algorithms proposed in [9][10] may be simplified for user authentication in our scheme. Different authentication methods generate different levels of access rights both for internal content and Internet based content. Usernames and their corresponding passwords needed for such accesses are grouped and stored in smart card, and are managed by the following proposed security protocol.

Generation of *Active Usage Level* (AUL) according to authentication method: When a user authenticates to the mobile device, an *active usage level*, denoted as AUL, is generated by the following method according to the method of authentication employed (for example as shown in Table 1.)

$$AUL = \begin{cases} \text{L2, if fingerprint,} \\ \text{L3, if L3 password,} \\ \text{L4, if L4 password,} \\ \text{L5, if no password.} \end{cases} \quad (1)$$

In this example, only L2 to L5 of active usage levels can be generated at the authentication time. AUL=L1 is never generated. The contents, services or applications of L1 can be accessible only by users whose AUL is L2. When a L2 user tries to access any item of level L1, the L1 password is asked (in case of L2 time out, a finger print scan is again requested.) After correctly giving L1 password, the user can access the L1 level content. As soon as the access to the applied item is terminated, the user returns back to AUL=L2.

Access contents, services and applications: After a user is authenticated to the devices with an active usage level AUL, she/he can access all contents, services and applications having security level AUL or lower. If the requested contents, services and applications are within the device and are of security level AUL or lower, the access rights are granted seamlessly without asking the user to again authenticate even though they are password-protected. If the user requests content, or services via any network and the requested contents/services are of security level L, at first L is compared with AUL. If L is less than or

equal to AUL, then the contents/services are accessed by executing corresponding authentication protocol without user interaction. Otherwise the user needs to authenticate again to gain higher active usage level or the request is denied.

Deal with other party's access: If a networked other party tries to access the protected contents and information inside the mobile device, it will first ask the other party to authenticate with username and password. The user can define own access group for authentication, or use standard authentication infrastructures for authenticating the other parties.

Re-authentication: If an authenticated user leaves the mobile device unused for a time out period T, which should ideally depend on the current AUL, the active usage level of the user is automatically decreased to AUL=L5, the lowest level. User can also reset the active usage level to L5 at any time. That is,

$$AUL = \begin{cases} \text{L5, if no key pressed in T,} \\ \text{L5, if user resets.} \end{cases} \quad (2)$$

To regain higher active usage level, the user needs to again authenticate using the specific method corresponding to that active usage level.

For security reason, if authentication using L3 or L4 password is failed for K times, that authentication method can be locked. To activate locked authentication method again, it can be made necessary to gain higher-level AUL (for example L2.)

Automatic password update: If user sets expiry dates for passwords, at the expiration of a password, a reminder will come up. After authenticated by using fingerprint and L1 password, user can activate automatic password update, which accesses the password server and automatically generate a new password. In order to improve password security, some password generation rules such as the password generation method proposed in [9] can be used. New password is updated to smart card. The password generated in this way is random and difficult to be attacked.

IV. Implementation

The best implementation is authentication middleware in a mobile device, which interacts with APIs of application layer and device control functions. Whenever an application or file/data access is requested, this authentication middleware is called.

In preparation, a user authenticates to access her/his mobile device, classifies all applications, files and data according to Table 1 and based on their importance. The usernames and passwords necessary for web accounts accesses are grouped and stored in smart card. Of course, user needs to obtain the corresponding level of AUL in order to put applications and files into the group of security L. In fact, most of the classifications are done when files or web accounts are created. After the device is powered up, the AUL is set to L5 in initialisation. Without authentication, user can still access free contents and applications grouped in L5. However, for accessing securer contents and applications, authentication to gain higher AUL is needed. Figure 1 shows the flowchart of generating AUL according to authentication methods.

The N and i for counting the failures of password and fingerprint authentication are set to zero at first power up. The algorithms for password and fingerprint verifications can be chosen from any standards or use the algorithms proposed in [6]-[10]. For password authentication, there are maximum k-1 successive failures allowed; otherwise it will be locked. The lock information and the number N for counting the failures are stored in specific addresses of flash memories, so that if the password authentication is locked, user cannot use password for authentication even she/he powers down and powers up the mobile device. N is set to zero after every successful password authentication, and the locked password authentication is unlocked after successful fingerprint verification. Fingerprint authentication will not be locked because an illegal user will not have the same fingerprint as the owner. In all cases, if authentications fail, the AUL is set to L5 and the application returns.

For the timer value T to reset AUL to L5 when there is no key input, it is changed to T2 or T3 and the timer is enabled after successful fingerprint or password authentication, and the timer value is reloaded each time a key is pressed.

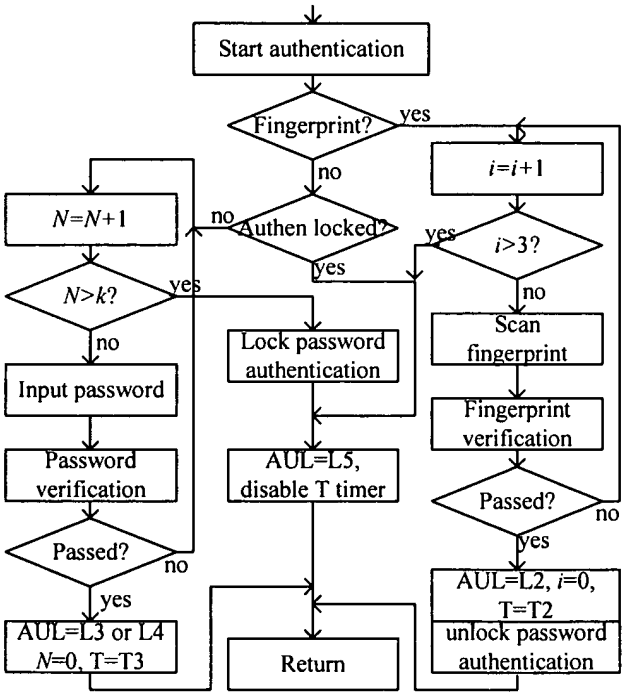

Figure 1. Authentication to gain access to mobile devices

Figure 2 depicts the flowchart of real time access control for both internal and Internet contents. The flowchart reflects the novel authentication and access control scheme proposed in this paper. In Figure 2, the blocks with "Ask for authentication" call for authentication process shown in Figure 1. For applications, files and data that belong to L1, the users have to first authenticate to gain AUL=L2, followed by L1 password verification. This is done on the left side of the flowchart.

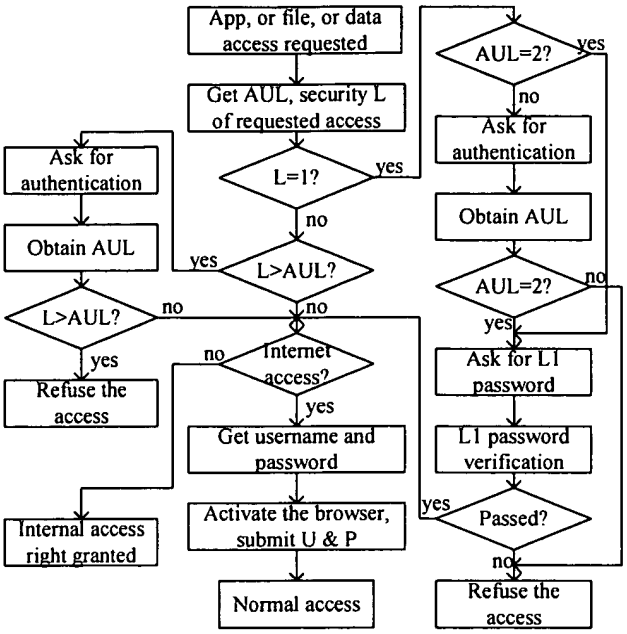

Figure 2. Novel authentication scheme

The AUL can be set to L5 either by interruption of timeout of timer T or by special key input from the user.

User can execute the automatic password updates at any time. However, if there is expiry dates set previously for passwords, there will be a notification come up upon expiry of the passwords. The flowchart of password automatic update is illustrated in Figure 3. Figure 3(a) is the function called by interruption of password expiration. Figure 3(b) is application for password update activated by user at any time. Figure 3(c) is the updating flowchart for all passwords. At first, it calls the novel authentication scheme shown in Figure 2 to check the fingerprint and L1 password. If authentication is successful, then it updates the password one-by-one for all web accounts from L1 to L4.

If a networked third party wants to access the contents inside the mobile terminal, which is protected in groups L2 to L4, authentication is necessary. Normally, such access is limited only to a small group of people who are close to the owner of the mobile terminal. Therefore, the owner can define an access group and authenticate them by consulting the access group. If a large number of persons needed to access the mobile device, the standard authentication infrastructure can be used.

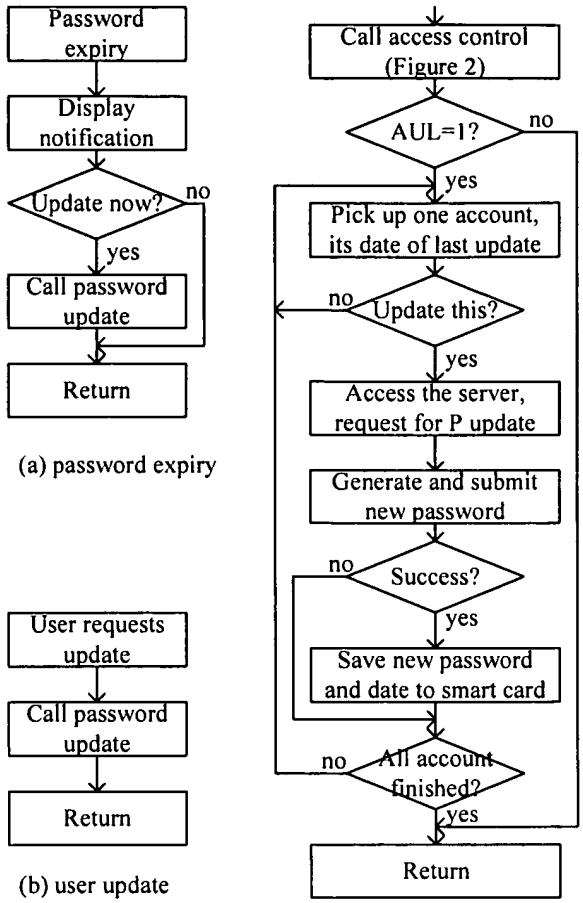

Figure 3. Automatic passwords update

V. SECURITY ANALYSIS

Unlike Persistent cookies [3], Liberty Identity Federation Framework (ID-FF) [4], Passport service and common password[5], our proposal does not need any modification in Internet servers or increasing interaction with any Internet servers. The modification and interaction with servers may degrade the security and privacy. In practical, our proposal is also good for privacy because all personal and sensitive information are well protected and stored in smart card or in the mobile device. While accessing a web account, only information of that account is provided. It is also easy for the owner to control and to manage the personal information and privacy.

In the rest of this section, we analyse the security of our proposal in three situations: password attack, mobile device being temporally used by others, and loss of the mobile device.

A. Password attack

There are two types of password attacks: attack to access the mobile device and attack to access the web accounts managed

through the mobile device. For the former attack, since an average mobile device is not always connected to a network, a remote attacker has less chance to hack in compared with an always-connected terminal. Even if the mobile device is always connected, attackers are unlikely successful because L3 and L4 password authentications will be locked after K times of failures, and user can choose passwords that are difficult to guess because user needs remember only two or three passwords. In worst case, if a remote attacker gets access to the mobile terminal, he cannot gain access to items of L1 and L2 because they need much tougher authentication schemes like fingerprint verification. Therefore, our method is secure enough for mobile devices.

For attacks to access the web accounts managed through the mobile devices, since users do not need to remember these passwords, and since the passwords can be automatically changed frequently, they are more difficult to attack compared to passwords that are remembered by users. It is also more secure than persistent cookies, passport service and common password because passwords are frequently updated and the local identities for different accounts are independent of each other in our scheme.

B. Mobile device is temporarily used by others

For family member or friends temporally share the mobile device, the owner can give a suitable access level, which only allows accessing certain groups of information. Therefore, it will not cause security problem. Due to timeout mechanisms of active usage levels, and default AUL 5 offers no facilities for accessing secure content, misplaced mobile devices or temporarily borrowed devices are less prone to be exploited. Hence compared with existing methods mentioned in section 2, our protocol is more secure when the device is shared with other users.

C. Loss of the mobile device

If the mobile device is lost and an attacker obtains it, it suffers an off-line password attack. However, since authentications using L3 or L4 password will be locked if the authentication is failed for K times, and it needs fingerprint type of user specific authentication to activate the locked authentication methods, the security protection offered by proposed method is stronger. By any chance, even if the attacker succeeds in password attack within K trials, all the content she/he can access is limited to the level that is less than the cracked level.

It is possible for the users to keep an up to date copy of the smart card. Just in case that if the mobile device is lost, users can plug the copy of smart card in another mobile device to quickly change all the passwords by using the automatic password updating function. In such case, loss of the mobile device will not cause security problem to the protected information in web accounts.

VI. CONCLUSIONS

In this paper, we have proposed a new authentication and control scheme for accessing the content both in mobile devices and on Internet. User does not need to provide or remember usernames and passwords when she/he accesses web accounts from the mobile device once authentication to the device is done. We also analyzed the security performance of our scheme and compared it with existing persistent cookies, passport service and the common password method. The proposed scheme offers superior protection even if the device is misplaced or lost. The proposed authentication scheme will enable mobile centric communications to be more secure and easier.

VII. REFERENCES

[1] Sandhu, R., "Good-enough security," *IEEE Internet Computing*, Vol. 7, No. 1, pp 66-68, Jan.-Feb. 2003.

[2] Millett, L.I. and Holden, S.H., "Authentication and its privacy effects," *IEEE Internet Computing*, Vol. 7, No. 6, pp 54-58, Nov.-Dec. 2003.

[3] D. Kristol and L. Montuili, "HTTP State Management Mechanism," *IETF RFC 2965 (http://www.rfc-editor.org/rfc/rfc2965.txt)*, Oct. 2000.

[4] "Specifications of Liberty Alliance Project," *http://www.projectliberty.org/resources/specifications.php*.

[5] Luo, H. and Henry, P., "A common password method for protection of multiple accounts," *Proc. 14th IEEE Conf. on Personal, Indoor and Mobile Radio Communications (PIMRC), 2003*, Vol. 3, pp 2749-2754, 7-10 Sept. 2003.

[6] Mimura, M. Ishida, S. and Seto, Y., "Fingerprint verification system on smart card," *Proc. Intern. Conf. on Consumer Electronics (ICCE), 2002, pp 182-183*, 18-20 June 2002.

[7] Sanchez-Reillo, R. Mengibar-Pozo, L. and Sanchez-Avila, C., "Microprocessor smart cards with fingerprint user authentication," *Aerospace and Electronic Systems Magazine, IEEE*, Vol. 18, No. 3, pp 22-24, March 2003.

[8] Yoichi Seto, "Development of personal authentication systems using fingerprint with smart cards and digital signature technologies," *Proc. 7th Intern. Conf. on Control, Automation, Robotics and Vision, (ICARCV) 2002*, Vol. 2, pp 996-1001, 2-5 Dec. 2002.

[9] Xunhua Wang, Heydari, M.H. and Hua Lin, "An intrusion-tolerant password authentication system," *Proc. 19th Annual Computer Security Applications Conference*, pp 110-118, 2003.

[10] Wen-Shenq Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Trans. on Consumer Electronics*, Vol. 50, No. 1, pp251-255, Feb 2004.

[11] Mark D. Corner and Brian D. Noble, "Zero-Interaction Authentication," *Proc. MobiCom 2002*.

Terms used **automatic password protection** Found **6,860** of **171,143**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Software/modelware tutorials II: Smart modeling: smart modeling - basic methodology and advanced tools
Arvind Mehta
December 2000 **Proceedings of the 32nd conference on Winter simulation**
Publisher: Society for Computer Simulation International
Full text available: pdf(156.88 KB) Additional Information: full citation, abstract, references

The paper discusses how a complex simulation project can be executed efficiently and effectively following simple basic methodology, and using advanced modeling features provided by the simulation tool. The paper explains the methodology that should be followed for the successful outcome of a simulation project. The paper also discusses and illustrates some of the advanced modeling capabilities provided by a simulation tool "Witness", that enable the user to build complex models very quickly and ...

2 Managing information on-line: there are so many players you can't find the game boards or models for campus-wide information systems
Lida Larsen, MaryJac M. Reed, Ken Han
November 1995 **Proceedings of the 23rd annual ACM SIGUCCS conference on User services: winning the networking game**
Publisher: ACM Press
Full text available: pdf(636.88 KB) Additional Information: full citation, index terms

3 Use of an on-line, time-shared graphics system to design and document printed circuit boards
Leonard Marks
June 1976 **Proceedings of the 13th conference on Design automation**
Publisher: ACM Press
Full text available: pdf(1.44 MB) Additional Information: full citation, abstract, references, citings, index terms

A very advanced computer aided design system was recently put into operation at Martin Marietta's Orlando Division. Its purpose was to provide engineering personnel with a powerful tool for significantly lowering the cost and schedule time required to design and document complex printed circuit boards. This paper describes how the system is utilized and interfaced with related automated activities.

4 The role of the host computer in defending against P.C.s

Don Holden
September 1986 **Proceedings of the Northeast ACM symposium on Personal computer security**
Publisher: ACM Press
Full text available: pdf(868.30 KB) Additional Information: full citation, index terms

5 Client-side web scripting

Marco Fioretti
March 2002 **Linux Journal**, Volume 2002 Issue 95
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(22.66 KB) Additional Information: full citation, abstract, index terms

Personalize your web experience with a little Perl.

6 A functional microcomputer network

C. R. Carman
November 1982 **Proceedings of the 10th annual ACM SIGUCCS conference on User services**
Publisher: ACM Press
Full text available: pdf(326.95 KB) Additional Information: full citation, abstract, index terms

Bishop's, like many other small universities and colleges, is constantly striving to supply state of the art computing facilities to students, faculty, and the administration from very limited funds. The very advantageous cost/performance ratio of this network has allowed the university to obtain such facilities while remaining within budget constraints. The paper describes the computer network of microcomputers installed at Bishop's in the summer of 1981. The experience of the f ...

7 Internet data management (IDM): Learning query languages of Web interfaces

André Bergholz, Boris Chidlovskii
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**
Publisher: ACM Press
Full text available: pdf(253.16 KB) Additional Information: full citation, abstract, references

This paper studies the problem of automatic acquisition of the query languages supported by a Web information resource. We describe a system that automatically probes the search interface of a resource with a set of test queries and analyses the returned pages to recognize supported query operators. The automatic acquisition assumes the availability of the number of matches the resource returns for a submitted query. The match numbers are used to train a learning system and to generate classific ...

Keywords: hidden Web, learning, query operators, search interface

8 Application and analysis of the virtual machine approach to information system security and isolation

Stuart E. Madnick, John J. Donovan
March 1973 **Proceedings of the workshop on virtual computer systems**
Full text available: pdf(588.14 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is an important factor if the programs of independent and possibly malicious users are to coexist on the same computer system. In this paper we show that a combined virtual machine monitor/operating system (VMM/OS) approach to information

system isolation provides substantially better software security than a conventional multiprogramming operating system approach. This added protection is derived from redundant security using independent mechanisms that are inherent in the design ...

9 Protection and the control of information sharing in multics

Jerome H. Saltzer
July 1974 **Communications of the ACM**, Volume 17 Issue 7
Publisher: ACM Press

Full text available: pdf(1.75 MB) Additional Information: full citation, abstract, references, citings, index terms

The design of mechanisms to control the sharing of information in the Multics system is described. Five design principles help provide insight into the tradeoffs among different possible designs. The key mechanisms described include access control lists, hierarchical control of access specifications, identification and authentication of users, and primary memory protection. The paper ends with a discussion of several known weaknesses in the current protection mechanism design.

Keywords: Multics, access control, authentication, computer utilities, descriptors, privacy, proprietary programs, protected subsystems, protection, security, time-sharing systems, virtual memory

10 Mobile media sharing in large-scale events: beyond MMS

Giulio Jacucci, Antti Salovaara
November 2005 **interactions**, Volume 12 Issue 6
Publisher: ACM Press

Full text available: pdf(890.86 KB) html(13.06 KB) Additional Information: full citation, references, index terms

11 Protecting applications with transient authentication

Mark D. Corner, Brian D. Noble
May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**
Publisher: ACM Press

Full text available: pdf(294.40 KB) Additional Information: full citation, abstract, references

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

12 Biometric identification

Anil Jain, Lin Hong, Sharath Pankanti
February 2000 **Communications of the ACM**, Volume 43 Issue 2
Publisher: ACM Press

Full text available: pdf(677.32 KB) html(37.23 KB) Additional Information: full citation, references, citings, index terms

13 Integrating security in a large distributed system

M. Satyanarayanan
August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3
Publisher: ACM Press

Full text available: pdf(2.90 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

14 Content integration for e-business

Michael Stonebraker, Joseph M. Hellerstein
May 2001 **ACM SIGMOD Record , Proceedings of the 2001 ACM SIGMOD international conference on Management of data SIGMOD '01**, Volume 30 Issue 2
Publisher: ACM Press

Full text available: pdf(75.79 KB) Additional Information: full citation, abstract, references, citings, index terms

We define the problem of content integration for E-Business, and show how it differs in fundamental ways from traditional issues surrounding data integration, application integration, data warehousing and OLTP. Content integration includes catalog integration as a special case, but encompasses a broader set of applications and challenges. We explore the characteristics of content integration and required services for any solution. In addition, we explore architectural alternatives and discuss ...

15 The evolution of the DECsystem 10

C. G. Bell, A. Kotok, T. N. Hastings, R. Hill
January 1978 **Communications of the ACM**, Volume 21 Issue 1
Publisher: ACM Press

Full text available: pdf(1.92 MB) Additional Information: full citation, abstract, references, citings, index terms

The DECsystem 10, also known as the PDP-10, evolved from the PDP-6 (circa 1963) over five generations of implementations to presently include systems covering a price range of five to one. The origin and evolution of the hardware, operating system, and languages are described in terms of technological change, user requirements, and user developments. The PDP-10's contributions to computing technology include: accelerating the transition from batch oriented to time sharing computing systems; ...

Keywords: architecture, computer structures, operating system, timesharing

16 File servers for network-based distributed systems

Liba Svobodova
December 1984 **ACM Computing Surveys (CSUR)**, Volume 16 Issue 4
Publisher: ACM Press

Full text available: pdf(4.23 MB) Additional Information: full citation, references, citings, index terms, review

17 Trusted products evaluation

Santosh Chokhani
July 1992 **Communications of the ACM**, Volume 35 Issue 7

Publisher: ACM Press

Full text available: pdf(4.09 MB) Additional Information: full citation, references, citings, index terms, review

Keywords: TCSEC, covert channel analysis, integrity, security, trust

18 Protecting privacy using the decentralized label model

Andrew C. Myers, Barbara Liskov

October 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 4

Publisher: ACM Press

Full text available: pdf(294.13 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Stronger protection is needed for the confidentiality and integrity of data, because programs containing untrusted code are the rule rather than the exception. Information flow control allows the enforcement of end-to-end security policies, but has been difficult to put into practice. This article describes the decentralized label model, a new label model for control of information flow in systems with mutual distrust and decentralized authority. The model improves on existing multilevel s ...

Keywords: confidentiality, declassification, downgrading, end-to-end, information flow controls, integrity, lattice, policies, principals, roles, type checking

19 Automated systematic testing for constraint-based interactive services

Patrice Godefroid, Lalita J. Jagadeesan, Radha Jagadeesan, Konstantin Läufer

November 2000 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 8th ACM SIGSOFT international symposium on Foundations of software engineering: twenty-first century applications SIGSOFT '00/FSE-8**, Volume 25 Issue 6

Publisher: ACM Press

Full text available: pdf(1.06 MB) Additional Information: full citation, abstract, references, citings, index terms

Constraint-based languages can express in a concise way the complex logic of a new generation of interactive services for applications such as banking or stock trading, that must support multiple types of interfaces for accessing the same data. These include automatic speech-recognition interfaces where inputs may be provided in any order by users of the service. We study in this paper how to systematically test event-driven applications developed using such languages. We show how such applic ...

Keywords: constraint-based languages, interactive services, model checking, state explosion, state-space reduction, testing, verification

20 Reducing risks from poorly chosen keys

T. Lomas, L. Gong, J. Saltzer, R. Needhamn

November 1989 **ACM SIGOPS Operating Systems Review , Proceedings of the twelfth ACM symposium on Operating systems principles SOSP '89**, Volume 23 Issue 5

Publisher: ACM Press

Full text available: pdf(598.93 KB) Additional Information: full citation, abstract, references, citings, index terms

It is well-known that, left to themselves, people will choose passwords that can be rather

readily guessed. If this is done, they are usually vulnerable to an attack based on copying the content of messages forming part of an authentication protocol and experimenting, e.g. with a dictionary, offline. The most usual counter to this threat is to require people to use passwords which are obscure, or even to insist on the system choosing their passwords for them. In this paper we show alternati ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next